

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250570

(43)Date of publication of application : 17.09.1999

(51)Int.Cl.

G11B 20/10
H04N 7/16

(21)Application number : 10-048221

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.02.1998

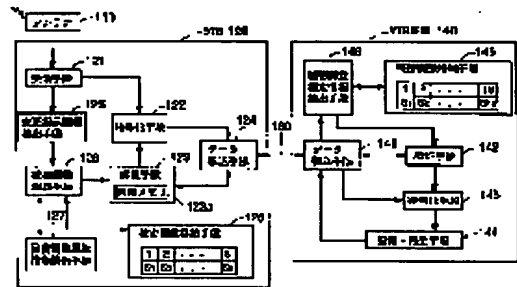
(72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) SECRET INFORMATION CHANGING SYSTEM, SECRET INFORMATION CHANGING FIRST DEVICE, SECRET INFORMATION CHANGING SECOND DEVICE, AND MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a secret information changing system, a secret information changing 1st device, a secret information changing 2nd device, and a medium in which demerit caused by eliminating an illegal device can be made less than a conventional device.

SOLUTION: A STB converting a received broadcasting radio wave to AV data and the like is provided with a receiving means 121, a change indication information detecting means 125 detecting only change indication information from a received signal, a secret function selecting means 128 adding contents of a secret function history information storing means 127 by indication of the change indication information detecting means 125, selecting a new secret function from a secret function storing means 126, and changing a secret function being used now to the other secret function, an authentication means 123 using the selected secret function, and the like, and a VTR device 140 connected with a transmitting line 160 is provided with a secret function indication information extracting means 146 detecting discrimination number information out of transmitted signals, extracting a corresponding secret function from a secret function storing means 145 and outputting it to an authentication means 142, a decoding means 143, and the like.



LEGAL STATUS

[Date of request for examination]

26.02.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-250570

(43) 公開日 平成11年(1999) 9月17日

(51) Int.Cl.⁶

G 1 1 B 20/10

H 0 4 N 7/16

識別記号

F I

G 1 1 B 20/10

H 0 4 N 7/16

H

A

審査請求 未請求 請求項の数18 O L (全 12 頁)

(21) 出願番号 特願平10-48221

(22) 出願日 平成10年(1998) 2月27日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 武智 秀明

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 松田 正道

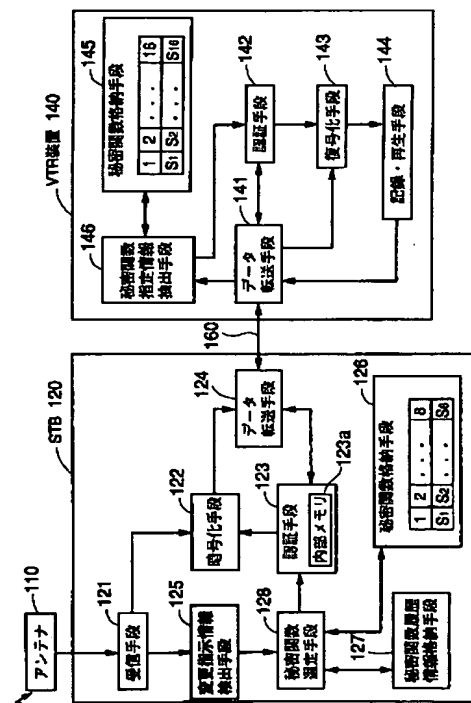
最終頁に続く

(54) 【発明の名称】 秘密情報変更システム、秘密情報変更第1装置、秘密情報変更第2装置、及び媒体

(57) 【要約】

【課題】不正装置の使用を阻止するために、悪用されたその秘密関数Sを使用しないようにすると、正規の装置までも使用出来なくなるという弊害があった。

【解決手段】受信した放送電波をAVデータ等に変換するSTBは、受信手段121と、受信信号から変更指示情報のみを検出する変更指示情報検出手段125と、変更指示情報検出手段125の指示で秘密関数履歴情報格納手段127の内容を加味して、秘密関数格納手段126から新たな秘密関数を選定し、現在使用中の秘密関数を別の秘密関数に変更する秘密関数選定手段128と、その選定された秘密関数を用いる認証手段123等を備え、伝送ライン160により接続されたVTR装置140は、伝送されてきた信号の中から識別番号情報を検出し、秘密関数格納手段145から対応する秘密関数を抽出し、認証手段142へ出力する秘密関数指定情報抽出手段146と、復号化手段143等を備える。



【特許請求の範囲】

【請求項1】 認証又は所定の処理に利用する第1秘密情報を、予め複数個有する第1装置と、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置とを備え、

前記第1又は第2装置が利用していた前記第1又は第2秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第1又は第2秘密情報を変更されるものであり、

前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更システム。

【請求項2】 認証又は所定の処理に利用する第1秘密情報を、予め複数個有する第1装置と、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置とを備え、

前記第1又は第2秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第1又は第2装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更システム。

【請求項3】 前記第2装置は、前記複数個の第2秘密情報の内、一部の第2秘密情報を有するものであり、前記第2装置により使用されていた第2秘密情報を変更すべき旨を伝える外部からの指示に基づいて、前記第2装置が、自らが有する前記第2秘密情報の中の、どの第2秘密情報に変更するかを選定するものであり、その第2装置が、前記選定結果に基づき、前記第1装置に対して前記第1秘密情報の変更を指示するものであることを特徴とする請求項2記載の秘密情報変更システム。

【請求項4】 前記第2装置が有する第2秘密情報の数が、前記第1装置が有する第1秘密情報の数と同じであり、

前記第1又は第2装置により使用されていた第1又は第2秘密情報を変更すべき旨を伝える外部からの指示があった場合は、前記第1又は第2装置が、自らが有する前記秘密情報の中の、どの秘密情報に変更するかを選定するものであり、且つ、その第1又は第2装置が、前記選定結果に基づき、前記第2又は第1装置に対して、前記第2又は第1秘密情報の変更を指示するものであること

を特徴とする請求項2記載の秘密情報変更システム。

【請求項5】 前記第1又は第2装置で利用される前記第1又は第2秘密情報を管理する管理装置を備え、前記外部からの指示は、前記管理装置から出される指示であり、且つ、その指示は、電波、又は電話回線を介して前記第1又は第2装置に送られることを特徴とする請求項1、3又は4記載の秘密情報変更システム。

【請求項6】 前記第1又は第2装置は、記録媒体を再生する再生手段を備え、

前記外部からの指示は、前記再生手段により再生される前記記録媒体中に記録された情報であることを特徴とする請求項1、3又は4記載の秘密情報変更システム。

【請求項7】 前記外部からの指示は、前記第1又は第2装置が有する第1又は第2秘密情報の内、秘密性が保持されなくなったものを除外した残りの秘密情報の中のどの秘密情報を利用すべきであるかという指示であることを特徴とする請求項1記載の秘密情報変更システム。

【請求項8】 前記第2装置は、前記複数個の第2秘密情報の内、一部の第2秘密情報を有するものであり、前記管理装置は、前記複数個の第1秘密情報の内、秘密性が保持されなくなったものを除外した残りの第1秘密情報の中から、どれかを採用して、それらを新たな第2秘密情報とすることを決定するものであり、

前記第2装置が有する前記一部の第2秘密情報は、前記決定に基づいて、前記新たな第2秘密情報により更新されたものであることを特徴とする請求項5記載の秘密情報変更システム。

【請求項9】 前記第2装置は、前記複数個の第2秘密情報の内、一部の第2秘密情報を有するものであり、前記管理装置は、前記複数個の第1秘密情報の内、秘密性が保持されなくなったものを除外した残りの第1秘密情報の中から、どれかを採用して、それらを新たな第2秘密情報とすることを決定し、その決定された新たな第2秘密情報を前記第2装置に送信するものであり、

前記第2装置は、前記送信されてきた新たな第2秘密情報により既に有していた前記第2秘密情報を更新することを特徴とする請求項5記載の秘密情報変更システム。

【請求項10】 前記第2装置は、前記複数個の第2秘密情報の内、一部の第2秘密情報を有するものであり、前記複数個の第1秘密情報の内、秘密性が保持されなくなったものを除外した残りの第1秘密情報の中から、どれかを採用して、それらを新たな第2秘密情報とすることを決定する管理装置を備え、

前記第2装置が有する前記一部の第2秘密情報は、前記決定に基づいて、前記新たな第2秘密情報により更新されたものであることを特徴とする請求項6記載の秘密情報変更システム。

【請求項11】 前記第2装置は、前記複数個の第2秘密情報の内、一部の第2秘密情報を有するものであり、前記複数個の第1秘密情報の内、秘密性が保持されなくな

ったものを除外した残りの第1秘密情報の中から、どれかを採用して、それらを新たな第2秘密情報とすることを決定し、その決定された新たな第2秘密情報を前記第2装置に送信する管理装置を備え、

前記第2装置は、前記送信されてきた新たな第2秘密情報により既に有していた前記第2秘密情報を更新することを特徴とする請求項6記載の秘密情報変更システム。

【請求項12】 前記再生手段により再生される記録媒体に、前記指示と矛盾する指示が記録されていた場合、その指示は無視されることを特徴とする請求項6記載の秘密情報変更システム。

【請求項13】 前記秘密情報は、前記データ送信装置と前記データ受信装置の間で、前記データの送信の前に行われる認証動作に利用する秘密関数、秘密鍵、又は公開鍵であることを特徴とする請求項1又は2記載の秘密情報変更システム。

【請求項14】 認証又は所定の処理に利用する第1秘密情報を、予め複数個有する秘密情報変更第1装置であって、

前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置又は、前記第1装置が利用していた前記第2又は第1秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第2又は第1秘密情報が変更されるものであり、

前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第1装置。

【請求項15】 認証又は所定の処理に利用するために第1装置が予め複数個有する第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第2装置であって、

前記第1装置又は前記第2装置が利用していた前記第1又は第2秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第1又は第2秘密情報が変更されるものであり、

前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第2装置。

【請求項16】 認証又は所定の処理に利用する第1秘密情報を、予め複数個有する秘密情報変更第1装置であって、

前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第

2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置の前記第2秘密情報又は、前記第1秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第2装置又は前記第1装置が、前記秘密情報をどれに変更するかを選定するものであり、

前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第1装置。

【請求項17】 認証又は所定の処理に利用するために第1装置が予め複数個有する第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第2装置であって、

前記第1秘密情報、又は前記第2秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第1装置又は前記第2装置が、前記秘密情報をどれに変更するかを選定するものであり、

前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものであることを特徴とする秘密情報変更第2装置。

【請求項18】 請求項1～17の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、秘密情報変更システム、秘密情報変更第1装置、秘密情報変更第2装置、及び媒体に関する。

【0002】

【従来の技術】従来より、衛星放送で送られてくるテレビ番組等を、専用の受信機（以下、これを単に、STBと呼ぶ）により受信して、そのSTBに接続されたVTR装置で録画したり、テレビで視聴したりすることが行われている。

【0003】この場合、放送されてくる映像・音声データの中には、例えば、記録が禁止されているものや、1回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。

【0004】そこで、STBから、例えばVTR装置に対して、1回のみ記録可能なAVデータを送信する場合、先ず、そのVTR装置が、上記の様な正規な装置であるかどうかを確認するための認証動作が行われることになると思われる。

【0005】以下に、従来のSTB及びVTR装置の構

成とその認証動作を簡単に述べる。

【0006】一般に、このようなSTBとVTR装置には、上記認証動作を行う為に用いる共通の秘密関数Sが、予め格納されている。

【0007】VTR装置からSTBに対して、AVデータの送信要求があると、上述したように、先ず、STBとVTR装置の間で、互いに上記秘密関数Sを用いて、次の様な、チャレンジ・レスポンス型認証と呼ばれる作業が行われる。

【0008】即ち、先ず、VTR装置からSTBに対して、リクエスト（認証要求）が出される。これを受けたSTBは、VTR装置に対して、チャレンジx（応答要求）を出し、VTR装置からの応答を待つ。又、STBは、自己の秘密関数Sを用いて、上記xからS(x)を生成する。尚、S(x)との記載は、xを秘密関数Sにより暗号化したものを表すものとする。

【0009】一方、VTR装置は、自己の秘密関数Sを用いて、受信したチャレンジxから独自にS(x)を生成し、そのS(x)をSTBへ送る。

【0010】STBは、自ら生成したS(x)と、VTR装置から送られてきたS(x)と比較して、一致すれば、VTR装置が正規な装置であると判定し、AVデータの送信を開始する。又、不一致であれば、VTR装置が不正な装置であると判定し、AVデータの送信は行わない。

【0011】尚、STBに複数の装置が接続されている場合、それら複数の装置が有する秘密関数は、全て同じである場合と、それぞれに固有のものである場合がある。後者の場合、STBは、それら装置に固有の全ての秘密関数を備えており、認証に際し、認証の相手装置に対応する秘密関数を使用するものである。

【0012】

【発明が解決しようとする課題】しかしながら、上記の様な認証方法では、不正者が、正規な装置の秘密関数Sをそっくりそのまま模倣して、上記と同じ認証方法を行える不正な装置を製造・販売し、その不正装置が使用された場合、上記認証方法では、その装置が不正な装置であることを見破ることが出来ない。そこで、仮に、秘密関数Sが不正者により悪用されていることが分かった場合、その不正装置の使用を阻止する対策としては、悪用されたその秘密関数Sを使用しないようにするしかない。そのため、使用が禁止された秘密関数Sを予め有している正規の装置までも使用出来なくなるという弊害が出るという課題があった。

【0013】本発明は、この様な従来の課題を考慮し、不正な装置の排除に伴う弊害を従来に比べてより少なく出来る秘密情報変更システム、秘密情報変更第1装置、秘密情報変更第2装置、及び媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】請求項1記載の本発明は、認証又は所定の処理に利用する第1秘密情報を、予め複数個有する第1装置と、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置とを備え、前記第1又は第2装置が利用していた前記第1又は第2秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第1又は第2秘密情報に変更されるものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更システムである。

【0015】請求項2記載の本発明は、認証又は所定の処理に利用する第1秘密情報を、予め複数個有する第1装置と、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置とを備え、前記第1又は第2秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第1又は第2装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更システムである。

【0016】請求項14記載の本発明は、認証又は所定の処理に利用する第1秘密情報を、予め複数個有する秘密情報変更第1装置であって、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置又は、前記第1装置が利用していた前記第2又は第1秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第2又は第1秘密情報に変更されるものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第1装置である。

【0017】請求項15記載の本発明は、認証又は所定の処理に利用するために第1装置が予め複数個有する第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第2装置であって、前記第1装置又は前記第2装置が利用していた前記第1又は第2秘密情報をどれに変更すべきであるかを伝える外部からの指示に基づいて、前記第1又は第2秘密情報に変更されるものであり、前記外部からの前記

指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第2装置である。

【0018】請求項16記載の本発明は、認証又は所定の処理に利用する第1秘密情報を、予め複数個有する秘密情報変更第1装置であって、前記複数個の第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う第2装置の前記第2秘密情報又は、前記第1秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第2装置又は前記第1装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第1装置である。

【0019】請求項17記載の本発明は、認証又は所定の処理に利用するために第1装置が予め複数個有する第1秘密情報に対応する複数個の第2秘密情報の内、全部又は一部の第2秘密情報を有し、その第2秘密情報を利用して、前記第1装置との間で前記認証を、又は前記所定の処理に対応する処理を行う秘密情報変更第2装置であって、前記第1秘密情報、又は前記第2秘密情報を変更すべき旨を伝える外部からの指示があった場合、前記第1装置又は前記第2装置が、前記秘密情報をどれに変更するかを選定するものであり、前記外部からの前記指示を受けた一方の前記装置が、他方の前記装置に対して、前記指示に基づく前記秘密情報の変更を指示するものである秘密情報変更第2装置である。

【0020】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0021】（第1の実施の形態）図1は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【0022】同図に示す様に、アンテナ110は、放送通信用衛星からの放送電波を受信する手段であり、衛星放送受信機（以下、これを単に、STBと呼ぶ）120は、受信した放送電波をAVデータ等に変換する手段である。この放送電波の中には、放送局（図示省略）が放送する通常のテレビ番組の他に、現在使用中の秘密関数を別の秘密関数に変更せよという内容の変更指示情報の放送も含まれている。この変更指示情報の放送は、秘密関数を管理している管理センター（図示省略）の指示の基に行われるものである。管理センターは、不正者によりある秘密関数が盗まれたという情報を得て、その秘密関数の秘密性が保持されなくなったと判断した場合に、

この様な変更指示情報を放送するものである。又、この変更指示情報には、上記盗まれた秘密関数を使用中の装置の固有のID情報が付されている。尚、秘密関数は、各装置間の認証作業において使用されるものであり、これについては、更に後述する。

【0023】伝送ライン160は、STB120とVTR装置140との間に設けられた伝送のためのバスラインである。

【0024】次に、同図を参照しながら、STB120の内部構成について更に述べる。

【0025】即ち、受信手段121は、アンテナ110と直結し、受信したデータの復調を行い、その受信データに施されている放送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。この受信データの中には、上述した変更指示情報が含まれている。尚、この変更指示情報の放送は、本実施の形態の様に他の番組放送の電波と多重化されていても良いが、単独で放送されてきても良い。

【0026】変更指示情報検出手段125は、受信手段121から出力される信号の中から、自己の固有のID情報が付された変更指示情報のみを検出し、変更指示情報を検出した旨を秘密関数選定手段128に出力する手段である。秘密関数格納手段126は、8個の秘密関数S1～S8を予め格納している手段である。又、これら秘密関数S1～S8には、それぞれに対応する1～8の識別番号が与えられているものとする。秘密関数履歴情報格納手段127は、使用が禁止された秘密関数及び現在使用中の秘密関数の識別番号を格納する手段である。秘密関数選定手段128は、変更指示情報検出手段125からの指示を得て、秘密関数履歴情報格納手段127の内容を加味して、現在使用中の秘密関数を別の秘密関数に変更する手段である。即ち、秘密関数選定手段128は、秘密関数格納手段126から新たな秘密関数の一つを選定し、その秘密関数をその識別番号とともに読み出し、それらを秘密関数指定情報として認証手段123へ送る手段である。又、秘密関数選定手段128は、秘密関数履歴情報格納手段127の内容を更新する手段である。

【0027】一方、暗号化手段122は、認証手段123からの指示に基づいて、予め備えた暗号化のためのワークキーKwにより、受信手段121から出力されてきたAVデータを圧縮状態のまま暗号化し、又、認証手段123により生成されたサブキーKsubを用いて、ワークキーKwを暗号化する手段である。サブキーKsubについては、後述する。尚、ここで、上記の様に暗号化されたワークキーKwをも端末装置へ送る必要があるのは、端末装置では、転送されてきたAVデータを復号化した上で、記録等することを前提としているからである。

【0028】認証手段123は、AVデータの転送要求

を行ったVTR装置との間で、VTR装置が正規の装置であるかどうかを確かめる認証作業を、上記秘密関数指定情報に基づいて行う手段である。認証手段123は、上記認証を始める際に、上記秘密関数指定情報に含まれる識別番号の情報を、認証相手となるVTR装置140へ送る手段である。

【0029】データ転送力手段124は、デジタル・インタフェースとして知られているIEEE1394である。データ転送手段124は、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない認証用データやコマンド等の転送に適したアシンクロナス転送の2つの転送を行う手段である。

【0030】次に、図1を参照しながら、VTR装置140の内部構成について、更に述べる。

【0031】同図に示すとおり、データ転送手段141は、データ転送手段124と同様のデジタル・インタフェースである。

【0032】秘密関数格納手段145は、16個の秘密関数S1～S16を予め格納している手段である。又、これら秘密関数S1～S16には、それぞれに対応する1～16の識別番号が与えられているものとする。尚、これら秘密関数S1～S8は、上述した秘密関数格納手段126が有する秘密関数と、識別番号も含めて同じである。秘密関数指定情報抽出手段146は、伝送されてきた信号の中から識別番号情報を検出し、それを基に、秘密関数格納手段145から対応する秘密関数を抽出し、認証手段142へ出力する手段である。

【0033】認証手段142は、秘密関数指定情報抽出手段146からの指示に基づいて、認証作業を行う手段である。又、認証手段142は、認証手段123が生成するものと同じのサブキーKsubを生成し、復号化手段143へ出力する手段である。復号化手段143は、データ転送手段141から得た暗号化されたワークキーKwをサブキーKsubにより復号化してワークキーKwを復元し、そのワークキーKwにより、暗号化されたAVデータを復号化する手段である。記録・再生手段144は、復号化されたAVデータを記録し、又、その記録データを再生する手段である。ここで、本発明の第1装置は、VTR装置140に対応し、本発明の第2装置は、STB120に対応する。本発明の複数個の第1秘密情報は、秘密関数S1～S16に対応する。又、本発明の複数個の第1秘密情報に対応する複数個の第2秘密情報は、本実施の形態では、上記複数個の第1秘密情報と同一のものである。又、本発明の複数個の第1秘密情報に対応する複数個の第2秘密情報の内、一部の第2秘密情報は、秘密関数S1～S8に対応する。

【0034】以上の構成により、以下に、図1、図2(a)、(b)を参照しながら、本実施の形態の動作を述べる。

【0035】本実施の形態では、既に使用が禁止された秘密関数が2つあるという前提で説明する。図2

(a)、(b)は、秘密関数履歴情報格納手段の内容を示す模式図である。図2(a)では、既に使用が禁止された秘密関数S1、S2の識別番号が、1と2であること、そして、その禁止された時間的順番が、識別番号1、2の順番であることを示し、又、現在使用中の秘密関数S3の識別番号が3であることを示している。

【0036】ステップ101：即ち、STB120とVTR装置140との間で、現在使用されている秘密関数S3が、不正者により盗まれたという情報を得た管理センターは、そのSTB120の固有のID情報を付した変更指示情報を放送するよう所定の放送局へ指示する。

【0037】ステップ102：放送局が、上記変更指示情報を、現在放送中の通常の放送番組と多重化して放送し、その通常の放送番組の後、引き続き通常の放送番組A、B、Cを多重化して放送する。

【0038】ステップ103：STB120のアンテナ110で受信された放送データは、受信手段121により上記所定の処理が行われ多重化が分離されて暗号化手段122と変更指示情報検出手段125へ出力される。

【0039】ステップ104：変更指示情報検出手段125は、受信手段121から出力されてくる信号の中に、自己の固有のID情報が付された変更指示情報があるかどうかをチェックする。ここでは、自己のID情報が付された変更指示情報の存在を検出するので、その旨を秘密関数選定手段128へ出力する。変更指示情報検出手段125より上記出力を得た秘密関数選定手段128は、先ず、秘密関数履歴情報格納手段127の内容

(図2(a)参照)を読み出して、秘密性が確保できなくなった秘密関数の識別番号が1～3であることを把握する。次に、秘密関数格納手段126(図1参照)から、上記識別番号1～3の秘密関数を除く、残りの秘密関数の中から識別番号が4の秘密関数S4を選定し、それらを読み出して、秘密関数指定情報として認証手段123へ出力する。この秘密関数指定情報により、認証手段123では、内部メモリ123aに保持されている秘密関数S3とその識別番号3が、秘密関数S4とその識別番号4により更新される。尚、本実施の形態では、新たな秘密関数の選定は、上述の通り、秘密関数格納手段126の識別番号の昇順に行われる。又、秘密関数選定手段128は、上記選定の結果により、図2(b)に示す様に、秘密関数履歴情報格納手段127の内容を更新する。ここで、図2(b)は、図2(a)と比較すると、識別番号3の秘密関数が使用禁止の関数として加わり、新たに使用する秘密関数の識別番号が4である状況を示した図である。

【0040】ステップ105：一方、VTR装置140では、放送番組Aの録画を行うために、先ず、認証手段142が、データ転送手段141を介して、STB12

0に対し、リクエストを行う。本実施の形態での認証は、認証に使用する秘密関数が外部からの指示に応じて変更される点を除いて、上述したものと同一チャレンジ・レスポンス型認証である。

【0041】ステップ106：即ち、VTR装置140からリクエストを受けたSTB120のデータ転送手段124は、その内容を認証手段123へ送る。認証手段123は、これに対して、チャレンジxをVTR装置140へ送ると同時に、内部メモリ123aに記録されている識別番号4番を読み出して、識別番号情報として送る。チャレンジxは、乱数を発生させて生成される。

【0042】ステップ107：VTR装置140の秘密関数指定情報抽出手段146は、データ転送手段141に送信されてきた信号の中から、識別番号情報を検出し、その内容から識別番号として、4番という情報を読み取る。そして、その4番に対応する秘密関数S4を、秘密関数格納手段145から抽出し、認証手段142へ出力する。

【0043】ステップ108：認証手段142は、この様にして送られてきた秘密関数S4を利用して、上記チャレンジxからS4(x)を生成して、それをレスポンスとしてSTB120へ送る。又、認証手段142は、チャレンジxからサブキーKsub・xを生成し、復号化手段143に送る。

【0044】ステップ109：STB120の認証手段123では、内部メモリ123aに記憶された秘密関数S4を用いて独自に生成したS4(x)と、VTR装置140からのレスポンスのS4(x)と比較する。比較の結果、この場合は、同一であると判断されて、認証が成立する。又、STB120の認証手段123は、この様に認証が成立した結果、チャレンジxからサブキーKsub・xを生成する。このサブキーはステップ108で述べたものと同一である。

【0045】以降、認証が成立した後の動作（ステップ110～111）は、本実施の形態の特徴的な動作ではないので、簡単に述べる。

【0046】ステップ110：暗号化手段122は、認証成立の情報を認証手段123から得て、受信手段121から出力されてきた信号から放送番組Aのみを対象にワークキーKwで暗号化する。又、暗号化手段122は、ワークキーKwを、サブキーKsub・xにより暗号化する。そして、これら暗号化されたKw（放送番組AのAVデータ）と、Ksub・x（Kw）とをデータ転送手段124からVTR装置140へ送る。

【0047】ステップ111：復号化手段143は、得られたサブキーKsub・xを用いて、上記送られてきたKsub・x（Kw）を復号し、更に、復号されたKwを用いて、Kw（放送番組AのAVデータ）を復号する。復号化された放送番組AのAVデータは記録・再生手段144により記録される。

【0048】ところで、秘密関数S3を盗んだ不正装置（図示省略）から、上記ステップ105で述べたものと同様のリクエストが有った場合について簡単に述べる。

【0049】即ち、この場合、不正装置は、新たな秘密関数S4を知らないで、STB120からのチャレンジxに対する、レスポンスは、S3(x)しか生成できない。そのため、この様な装置からのレスポンスは、STB120が比較基準として用意している新たなS4(x)と一致せず、認証が不成立となる。従って、この様な装置には、要求データの転送は行われず、以降の処理が打ち切られる。これにより、不正装置のみを完全に排除出来る。

【0050】尚、管理センターからの変更指示が無い場合の、認証動作については、上記ステップ105～ステップ111と基本的に同じである。

【0051】次に、上記秘密関数S4が、不正者により盗まれたという情報を管理センターが得た場合における、上記とは別の動作を述べる。

【0052】管理センターは、秘密性が保持出来なくなり使用不可能となった秘密関数がある程度増えてくると、STB装置の製造メーカーに対して、次ロットのSTBの生産時からは、秘密関数格納手段126の内容を更新するように指示する。この指示を受けて、製造メーカーでは、次ロットのSTBを生産する場合、上記秘密関数S1～S16の16個の中から、既に使用不可能となった秘密関数S1～S4を除く、8個の秘密関数を新たに選定し、その識別番号と共に秘密関数格納手段126へ格納する（図3(a)参照）。図3(a)は、次ロットとして生産されるSTBが内蔵する秘密関数格納手段の内容を示す模式図である。図3(b)は、既に生産されたSTBが内蔵している秘密関数格納手段の内容を示す模式図である。尚、この様に、STBが内蔵する秘密関数格納手段の内容が更新されても、その更新が、あくまで、既に生産されたVTR装置に予め格納されている秘密関数の範囲内であるので、既存のVTR装置が使用できなくなるという問題は生じない。又、この様に、STBが内蔵する秘密関数格納手段の内容を所定のタイミングで更新することにより、STBをも、管理センターの管理下に置くことが出来得る。即ち、ここでは、STBが不正装置である場合までは想定していないが、STBをこの様に管理センターの管理下に置くことにより、例えば、管理センターからの変更指示に従わず、使用禁止の秘密関数を使用し続ける様な不正なSTBが発生しにくい環境にすることが出来る。

【0053】尚、上記実施の形態では、秘密関数格納手段126の内容の更新を、新たな装置の製造段階で行う場合について述べたが、これに限らず例えば、既存の装置に対して、新たな秘密関数を管理センターからの指示により放送局から放送波で送り、それを基に更新が行われる構成でも良い。この場合、図1における、受信手段

121及び変更指示情報検出手段125等が、上記機能に加えて、次の様な機能を有している必要がある。即ち、先ず、放送局から、秘密関数のデータを有する更新指示情報が放送されてくる。ここでは、更新指示情報の内容が、図3(a)に示すものと等価であり、秘密関数格納手段126の内容が図3(b)と同じである場合を例として述べる。受信手段121は、この更新指示情報を受信し、他の放送データと分離して出力する。変更指示情報検出手段125は、受信手段121の出力から更新指示情報を検出し、その更新指示情報に含まれている秘密関数S5～S12とその識別番号5～12を抽出する。更に、その抽出した秘密関数とその識別番号により、秘密関数格納手段126の内容(図3(b)参照)を更新する。その結果、秘密関数格納手段126の内容は、図3(a)に示した内容となる。その他の構成は、図1で述べたものと同様である。

【0054】(第2の実施の形態)図4は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【0055】尚、本実施の形態では、STB400とDVDプレーヤー420とにより構成される秘密情報変更システムについて述べるが、図1で説明したものと同一のものには、同一の符号を付し、その詳細な説明を省略する。従って、ここでは、上記実施の形態との相違点を中心に述べる。本実施の形態における上記実施の形態との主な相違点は、次のような点である。

- (1) 変更指示情報が、DVDに記録されていること。
- (2) その変更指示の内容が、使用すべき秘密関数の識別番号を指定するものであること。
- (3) DVDプレーヤー420が、変更指示情報を検出し、秘密関数の選定を行うこと。
- (4) そのため、DVDプレーヤー内の秘密関数格納手段424が有する秘密関数の数の方が、STB内の秘密関数格納手段404が有する秘密関数の数よりも少ないこと。
- (5) DVDプレーヤー420によりDVDからデータを読み出して、STB400に接続されたモニター410で視聴する場合であって、不正なSTBを排除することを想定していること。

【0056】図4に示すように、STB400とDVDプレーヤー420は、データ転送手段405及び425により伝送ライン160を介して接続されている。データ転送手段405及び425は、上記実施の形態と同様、何れもIEEE1394により構成されている。

【0057】又、同図に示すように、DVDプレーヤー420の構成は、ドライブ421、データ解読手段422を新たに備えるなど下記の点を除いて、図1に示すSTB120と共通する。

【0058】即ち、ドライブ421は、セットされたDVDを回転駆動し、記録信号を読み出す手段である。

又、データ解読手段422は、ドライブ421で読み出された信号からAVデータを解読する手段である。変更指示情報検出手段125は、ドライブ421より出力されてくる信号から変更指示情報を検出する手段である。

又、秘密関数抽出手段424は、秘密関数選定手段128とは異なり、変更指示情報により指示された識別番号を基に、秘密関数格納手段423から秘密関数を抽出する手段である。従って、ここでは、図1で示した秘密関数履歴情報格納手段127は不要である。又、秘密関数格納手段423は、図1で述べた秘密関数と異なる秘密関数S101～S108及びその識別番号101～108を格納する手段である。又、認証手段123は、内部メモリ123aに加えて、履歴メモリ123bを有している点は、図1と相違する。履歴メモリ123bは、使用が禁止された秘密関数の識別番号の履歴を記録する手段である。ここで、本発明の第1装置は、DVDプレーヤー420に対応し、本発明の第2装置は、STB400に対応する。又、本発明の再生手段は、ドライブ421等を含む手段である。

【0059】一方、同図に示すSTB400の構成について述べる。

【0060】即ち、秘密関数指定情報抽出手段406は、DVDプレーヤー420からの伝送信号の中から識別番号情報を検出し、それを基に、秘密関数格納手段404から対応する秘密関数を抽出し、認証手段401へ出力する手段である。又、復号化手段402は、認証手段401より送られてきたサブキーKsubを利用して、暗号化されたワークキーKwを復号化し、更に、それを用いて暗号化されたAVデータを復号化し、デコーダ403へ送る手段である。ここで、識別番号情報は、第1の実施の形態で述べたものと基本的に同じである。尚、デコーダ403を除く、これら各手段は、図1で述べたVTR装置140における各手段の内の同一名称の各手段と基本的に同じものである。但し、秘密関数格納手段404が格納する秘密関数とその識別番号は、図1で述べた秘密関数と異なる秘密関数S101～S116及びその識別番号101～116を格納する手段である。

【0061】又、デコーダ403は、復号化されたAVデータは、圧縮したままであるので、これを伸張し、その伸張した信号をモニター410へ出力する手段である。尚、アンテナ110及び受信手段121は、図1で述べたものと同じであるが、受信手段121の出力は、デコーダ403へ送られる点が異なる。

【0062】以上の構成において、次に、本実施の形態の動作を述べる。

【0063】ここでは、現在使用されている秘密関数S101が不正者により盗まれたという情報を得た管理セ

ンターが、次に製造するDVD₂に対しては、通常のAVデータ以外に、識別番号102の秘密関数を使用せよという内容の変更指示情報を記録する様に、DVDの製造メーカーに指示し、それが製造された場面を考える。そして、その新たなDVD₂が視聴される場合について説明する。

【0064】ステップ201：所望の映画を見るために、使用者がDVD₂をDVDプレーヤ420にセットして、駆動スイッチ（図示省略）をONする。これによりドライブ421が、DVD₂を回転駆動させ、変更指示情報が記録されているかどうかを最初にチェックし、記録されていれば、それを検出し、秘密関数抽出手段424へ出力する。ステップ202：秘密関数抽出手段424は、変更指示情報の内容を調べる。ここでは、識別番号102の秘密関数を使用せよという内容であるので、秘密関数格納手段423の中から、その識別番号102に対応する秘密関数S102を抽出する。抽出した秘密関数S102とその識別番号102とを認証手段123へ送る。

【0065】ステップ203：認証手段123が、この秘密関数抽出手段から送られてきた秘密関数S102とその識別番号102により、内部メモリ123aに記録されている現在使用中の秘密関数S101とその識別番号101番を更新する。更に、履歴メモリ123bに、使用が禁止された秘密関数の識別番号として、101番を追加記録する。履歴メモリ123bの利用については、後述する。

【0066】ステップ204：認証手段123が行う認証動作は、STB400が正規な装置であるかどうかを認証するものである。又、認証手段123と認証手段401との間で行われる認証動作は、ステップ106～109で述べたチャレンジ・レスポンス型認証とほぼ同じである。

【0067】但し、本実施の形態では、DVDプレーヤ420がSTB400に対してチャレンジxを送るものであり、第1の実施の形態の場合と、STBとその接続装置との立場が逆転している。又、その際、内部メモリ123aに記録されている識別番号102番を読み出して、識別番号情報としてチャレンジxと共に送る。

【0068】又、STB400の秘密関数指定情報抽出手段406は、上記ステップ107における秘密関数指定情報抽出手段146と同様の動作を行うが、ここでは、識別番号情報の内容が、識別番号102番を示すものであるので、秘密関数格納手段404の中から、それに対応する秘密関数S102を抽出し、認証手段401へ出力する。

【0069】又、認証手段401における、レスポンス及びサブキーKsub・xの生成は、上記ステップ108の内容と同じである。

【0070】又、DVDプレーヤ420の認証手段12

3における認証の成否判定及びサブキーKsub・xの生成は、上記ステップ109の内容と同じである。

【0071】ステップ205：認証が成立し、復号化手段402により復号化されたAVデータは、デコーダ403へ送られて、伸張処理されて、モニター410へ送られる。この様にして、使用者は、所望の映画を見ることが出来る。

【0072】これにより、上記実施の形態の場合と同様、不正装置のみを排除出来る。

【0073】次に、DVD₂と比較すると旧タイプとなるDVD₁を視聴する場合について、簡単に述べる。

【0074】このDVD₁には、識別番号101の秘密関数を使用せよという内容の変更指示情報が記録されているものとする。

【0075】この場合、ステップ203の述べた内部メモリ123aの更新の前に、次のような動作を行う。

【0076】即ち、認証手段123は、上記更新の前に、履歴メモリ123bの内容と、更新内容を比較する。ここでは、既に、履歴メモリ123bには、識別番号101は、使用禁止として記録されている。従って、既に使用が禁止されているものを復活させることになる判断し、この場合には、上記更新は行わず、その様な変更指示情報は無視する。

【0077】これにより、一旦、新タイプのDVDを再生させた後は、旧タイプのDVDを再生させる場合でも、秘密関数は、新しいものに維持できるので、不正装置の排除がより一層確実に出来るものである。

【0078】尚、本実施の形態においても、DVDプレーヤ420が内蔵する秘密関数格納手段423の内容を、製造メーカーにおいて、所定のタイミングで更新することは、第1の実施の形態で述べた場合と同様に行える。

【0079】（第3の実施の形態）図5は、本発明の一実施の形態における秘密情報変更システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の秘密情報変更システム及び各装置の構成について述べる。

【0080】本実施の形態では、STB500に対して、上記実施の形態で述べたものと同様のVTR装置140及びDVDプレーヤ420が、伝送ライン160を介して接続されている構成である。又、STB500は、上記実施の形態で述べたSTB120とSTB400の両方の機能を併せ持つ構成である。従って、上述したのと同じ構成のものには、同じ符号を付してその説明を省略する。

【0081】ここでは、上記実施の形態との相違点を中心に述べる。本実施の形態における上記実施の形態との主な相違点は、次のような点である。

（1）STB500が使用する秘密関数は、接続されている装置の種類によって異なるものであること。

(2) STB500の認証手段501は、データ送受信の相手との関係により、使用する秘密関数を指示する立場と、逆に指示される立場の両方の立場を使い分ける様に構成されていること。即ち、STB500からVTR装置140にAVデータを転送する場合の認証手段501は、その認証動作において、使用すべき秘密関数をVTR装置140に対し指示する立場となる。これに対して、DVDプレーヤ420から転送されてくる再生信号をモニター410に表示する場合の認証手段501は、その認証動作において、使用すべき秘密関数をDVDプレーヤ420から指示される立場となる。これらそれぞれの動作は、上記実施の形態で別々に述べたものと同様であり、ここでは省略する。

【0082】次に、管理センターの指示に基づき、放送局から、DVDプレーヤ420が使用する秘密関数の変更指示情報が有った場合について簡単に述べる。尚、この変更指示の内容は、使用すべき秘密関数の識別番号を指定する内容であるとする。

【0083】この変更情報は、STB500のアンテナ110を通り、受信手段121を経て、変更指示情報検出手段125に入ることは上述したものと同じである。変更指示検出手段125は、この変更指示の対象となる秘密関数が、STB500自身が主体的に変更出来る立場にあるものに該当するかどうかを予め定められた基準から判断する。そして、この秘密関数は、STB500自身が主体的に変更する立場にないものと判断して、上記変更指示情報は、データ転送手段405へ送られて、DVDプレーヤ420へ転送される。

【0084】本実施の形態のDVDプレーヤ420では、図4で示したデータ転送425と変更情報検出手段125の間に、図4では示していない信号の伝達ラインを新たに設けておくことにより、上記変更指示情報が変更指示情報検出手段125へ送られる。以降の動作は、ドライブ421から変更指示情報が出力されてきた場合と同様である。

【0085】このように、本実施の形態においても、上記の場合と同様の効果が発揮される。

【0086】ところで、上述した各実施の形態の何れか一つの実施の形態に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを磁気記録媒体や光記録媒体などの媒体に記録したものを作成し、それを用いて、上記と同様の動作を行わせても良い。

【0087】尚、上記実施の形態では、外部からの変更指示情報は、現在使用中のものを変更せよという場合、使用すべきものを指示してくる場合について述べたが、これに限らず例えば、使用すべき識別番号をアップせよ、換言すれば、使用すべき識別番号のバージョンナンバーをアップせよでもく、各装置内部はこれに対応する構成としても良い。但し、このような昇順タイプの構

成の場合、不正な指示を排除するため、例えば、現在使用中の識別番号が1番の時に、識別番号をいきなり8番にせよとの変更指示情報が有っても、これを無視し、識別番号2への変更ししかない様にしてもよい。

【0088】又、上記実施の形態では、STBと各装置との間で、それぞれが有する秘密関数の個数が、異なっている場合について述べたが、これに限らず例えば、個数は、双方とも同一でも良い。

【0089】又、本発明の第1又は第2秘密情報は、上記実施の形態では、認証に利用する秘密関数であったが、これに限らず例えば、認証に利用する秘密鍵又は公開鍵、その他、鍵の生成の元になる鍵の種的なものでもかまわない。

【0090】又、本発明の第1又は第2秘密情報は、上記実施の形態では、認証に利用する秘密関数であったが、これに限らず例えば、認証とは関係なく、転送すべきデータを暗号化するために使用するものであっても良い。この場合、認証手段は無くてもかまわない。

【0091】又、上記実施の形態では、認証方法として、チャレンジ・レスポンス型の認証であり、使用すべき秘密関数の指示は、チャレンジと同時にを行う場合について述べたが、これに限らず例えば、別のタイプの認証方法でもよく、又、認証方法の如何に関わらず、使用すべき秘密情報の指示を行うのは、秘密情報の変更に対して主導権を持っている装置である。

【0092】又、上記実施の形態では、本発明の第1秘密情報と第2秘密情報が同じである場合について述べたがこれに限らず例えば、同一でなくても勿論良い。

【0093】

【発明の効果】以上述べたところから明らかなように本発明は、不正な装置の排除に伴う弊害を従来に比べてより少なく出来るという長所を有する。

【図面の簡単な説明】

【図1】本発明の一実施の形態における秘密情報変更システムの構成を示す構成図

【図2】(a)、(b)：同実施の形態における、秘密関数履歴情報格納手段の内容を示す模式図

【図3】(a)：本実施の形態における、次ロットとして生産されるSTBが内蔵する秘密関数格納手段の内容を示す模式図

(b)：本実施の形態における、既に生産されたSTBが内蔵している秘密関数格納手段の内容を示す模式図

【図4】本発明の第2の実施の形態における秘密情報変更システムの構成を示す構成図

【図5】本発明の第3の実施の形態における秘密情報変更システムの構成を示す構成図

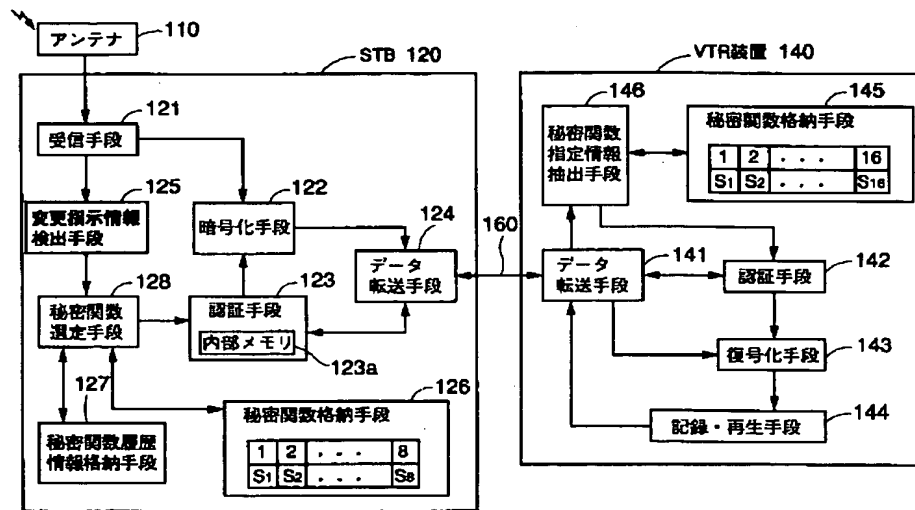
【符号の説明】

| | |
|-----|-------|
| 110 | アンテナ |
| 120 | STB |
| 140 | VTR装置 |

160 伝送ライン
 125 変更指示情報検出手段
 121 受信手段
 126 秘密関数格納手段

127 秘密関数履歴情報格納手段
 128 秘密関数選定手段
 123 認証手段
 122 暗号化手段

【図1】



【図2】

(a)

| 現在使用中の 秘密関数の識別番号 | 使用が禁止された 秘密関数の識別番号 |
|---------------------|-----------------------|
| 3 | 1 |
| | 2 |
| | |

(b)

| 現在使用中の 秘密関数の識別番号 | 使用が禁止された 秘密関数の識別番号 |
|---------------------|-----------------------|
| 4 | 1 |
| | 2 |
| | 3 |
| | |

【図3】

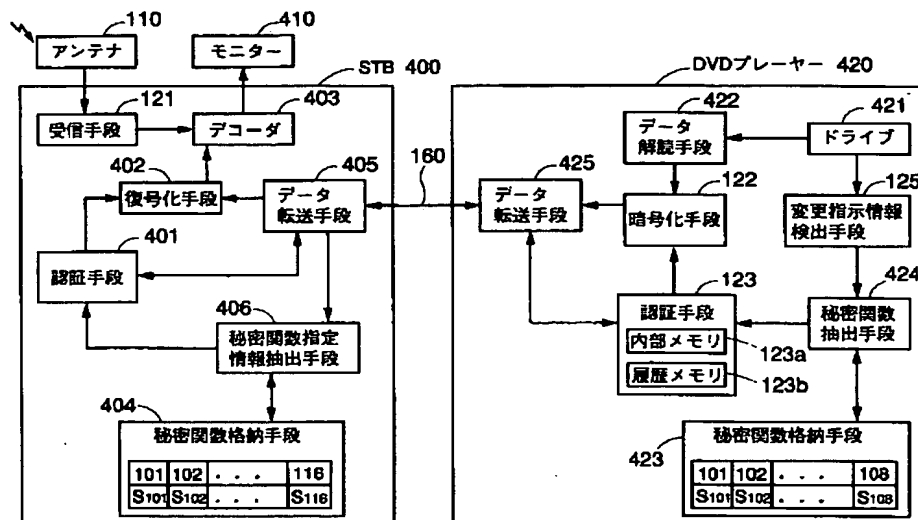
| 識別番号 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|------|----------------|----------------|----------------|----------------|----------------|-----------------|-----------------|-----------------|
| 秘密関数 | S ₅ | S ₆ | S ₇ | S ₈ | S ₉ | S ₁₀ | S ₁₁ | S ₁₂ |

(a)

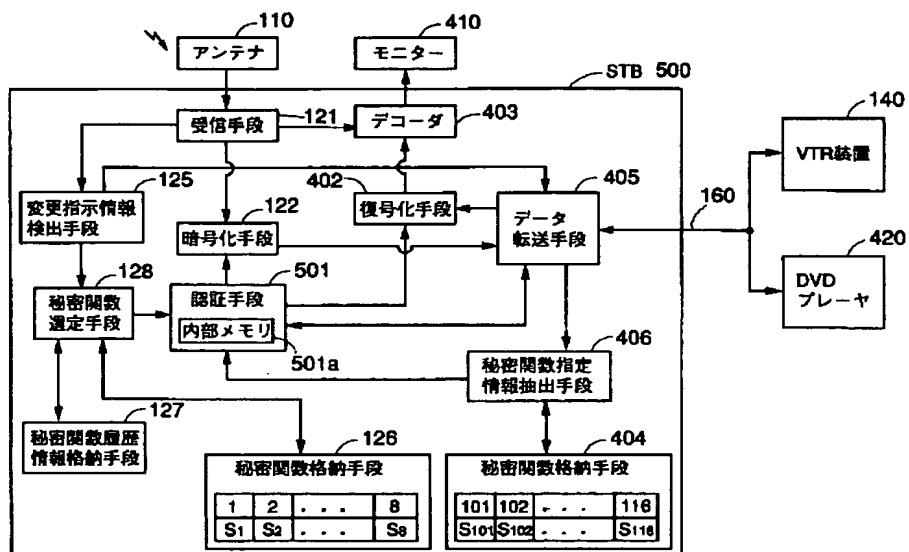
| 識別番号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| 秘密関数 | S ₁ | S ₂ | S ₃ | S ₄ | S ₅ | S ₆ | S ₇ | S ₈ |

(b)

【図4】



【図5】



フロントページの続き

(72)発明者 後藤 昌一
大阪府門真市大字門真1006番地 松下電器
産業株式会社内